11-01-00 A

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80528-9599

PATENT APPLICATION

ATTORNEY DOCKET NO. 10992596-1

10/30/00 EC982 U.S. PTO

IN THE U.S. PATENT AND TRADEMARK OFFICE
Patent Application Transmittal Letter

jc915 U.S. PTO 09/702183 10/30/00

ASSISTANT COMMISSIONER FOR PATENTS
Washington, D.C. 20231

Sir:

Transmitted herewith for filing under 37 CFR 1.53(b) is a(n): (X) Utility ( ) Design
(X) original patent application,
( ) continuation-in-part application

INVENTOR(S): **Keith E. Moore**

TITLE: **Document Authentication Using the Physical Characteristics of Underlying Physical Media**

Enclosed are:

(X) The Declaration and Power of Attorney. (X) signed ( ) unsigned or partially signed

(X) 5 sheets of drawings (one set) ( ) Associate Power of Attorney

( ) Form PTO-1449 ( ) Information Disclosure Statement and Form PTO-1449

( ) Priority document(s) ( )(Other) _____ (fee $_____)

CLAIMS AS FILED BY OTHER THAN A SMALL ENTITY				
(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) TOTALS
TOTAL CLAIMS	17 — 20	0	X $18	$ 0
INDEPENDENT CLAIMS	3 — 3	0	X $78	$ 0
ANY MULTIPLE DEPENDENT CLAIMS	0		$260	$ 0
BASIC FEE: Design $310.00); Utility $690.00)				$ 690
TOTAL FILING FEE				$ 690
OTHER FEES				$
TOTAL CHARGES TO DEPOSIT ACCOUNT				$ 690

Charge $ 690 to Deposit Account 08-2025. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16, 1.17,1.19, 1.20 and 1.21. A duplicate copy of this sheet is enclosed.

"Express Mail" label no. EL188087758US

Date of Deposit 10/30/00

I hereby certify that this is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231.

By _____

Typed Name: **Tiffany Turner**

Respectfully submitted,

Keith E. Moore

By _____

Thomas X. Li

Attorney/Agent for Applicant(s)
Reg. No. **37,079**
Date: **10/30/00**

Telephone No.: **(650) 857-5972**

Rev 12/99 (TransNew)

- Attach as First Page to Transmitted Papers -

UNITED STATES PATENT APPLICATION FOR

DOCUMENT AUTHENTICATION USING THE PHYSICAL CHARACTERISTICS OF UNDERLYING PHYSICAL MEDIA

Inventor:
Keith E. Moore

BACKGROUND OF THE INVENTION

Field of Invention

The present invention pertains to the field of document authentication. More particularly, this invention relates to document authentication using the physical characteristics of the underlying physical media of the document.

Art Background

A wide variety of documents including event tickets, paper currency, stock certificates, securities, checks, and other legal documents, etc., are commonly subject to various types of forgery. For example, such documents may be copied using color copiers. In another example, ink may be stripped off of the paper which underlies an authentic document and a new image printed on the paper, thereby enabling conversion of a low face value document to a high face value document.

In some prior methods of document authentication, a water-mark and/or other object is inserted into the paper on which a document is printed. Such methods attempt to avoid forgeries by making it difficult to reproduce the characteristics of the paper which underlies a document. Unfortunately, such methods usually cannot prevent the stripping of ink from the original paper and the printing of a new image.

SUMMARY OF THE INVENTION

A method for authenticating a document is disclosed in which a document key for the document is generated by examining one or more attributes of a physical media that underlies the document. An original image is then imparted onto the physical media so that the original image is associated with the document key in a way that enables a subsequent recovery of the document key from the original image. This tying together of the underlying physical media, through the document key, with an original image enables detection of a forgery which was performed either through an alteration of the original image, or ink stripping and re-printing, or a printing of the original image on another physical media.

Other features and advantages of the present invention will be apparent from the detailed description that follows.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is described with respect to particular exemplary embodiments thereof and reference is accordingly made to the drawings in which:

Figure 1 shows a method for authenticating a document according to the present techniques;

Figure 2 shows a method for digitally signing a document to impart the document key onto the physical media of a document according to the present techniques;

Figure 3 shows a method for verifying a document according to the present techniques;

Figure 4 shows one possible arrangement for generating a document key for a document;

Figure 5 shows one possible arrangement of predetermined areas of a document which are examined when generating a document key.

DETAILED DESCRIPTION

Figure 1 shows a method for authenticating a document according to the present techniques. The document authenticated may be any conceivable document including event tickets, paper currency, stock certificates, securities, checks, and other legal documents, etc., to name a few examples.

At step 10, a document key for the document is generated. The document key is based on one or more unique physical attributes associated with the physical media which underlies the document. The physical media is commonly paper media but the present teachings apply equally well to other types of underlying materials.

In some embodiments, the unique physical attributes upon which the document key is based are the random differences in the density and/or orientation of the paper fibers that were formed during the manufacture of the paper media which underlies the document. One known arrangement for determining the random differences in the density and/or orientation of paper fibers is described in U.S. Patent No. 5,089,712. Other known mechanisms that enable detection of paper fiber characteristics may also be employed.

Alternatively, the unique physical attributes may be a unique pattern printed in the paper media such as through the use of a reflective substance or UV ink or predetermined shapes printed in

predetermined positions. The predetermined positions or locations may be measured and encoded in a digital key at the time the image is created/locked. The location may be measured relative to an element of an image printed on the media.

At step 12, an original image is imparted onto the physical media that underlies the document. The original image is imparted so that the document key may be subsequently recovered from the original image. Step 12 may be performed by encoding the document key into the original image. The document key may be encoded using digital signing techniques. Alternatively, step 12 may be performed by encoding the document key (using a private key for example) and printing the encoded document key, which is a number, on the physical media that underlies the document.

Figure 2 shows a method for digitally signing a document to impart the document key onto the physical media of a document according to the present techniques. At step 14, a digital signature for the document is generated. The digital signature is generated using the document key obtained at step 10 and a private key which is allocated to the document. The digital signature may be generated using any known digital signing technique. For example, the document key from step 10 may be used as a public key and a public-private key mechanism may be used to generate the digital signature.

At step 16, the digital signature obtained at step 14 is encoded into an original image on the document. Step 16 ties an original image on the document to the underlying physical media, via the document key, so that copying the original image to a different paper with different unique physical attributes breaks the tie.

The digital signature may be encoded in the dithering patterns of an original image which is printed on the physical media. The encoding technique may be based on an encoding matrix for a grey pattern or color pattern. Alternatively, the digital signature may be printed on the paper as a number.

In yet another alternative, the digital signature may be embedded in the paper using a digital watermark. It may be preferable that only a portion of the total image be watermarked. In this manner, a watermark is recoverable even if a portion of the document is damaged. The only portion which must not be damaged is the section wherein the document key was encoded/read such as the square in which the paper fibers are read. This level of redundancy allows the paper to be handled without invalidating the document key and the watermark.

Figure 3 shows a method for verifying a document according to the present techniques. At step 20, a document key for the document being verified is generated. The document key is based on the unique physical attributes of the physical media which

underlies the document being verified. The document key is obtained at step 20 in a manner similar to that used in step 10, i.e. the same unique attributes are examined at step 20 when verifying a document as were examined at step 10 when authenticating the document.

At step 24, a recovered document key, the document key which was imparted onto the document at step 12, is recovered from the original image. The recovery of a document key at step 24 is essentially the reverse of the process used at step 12. For example, if the document key was incorporated into a digital signature which was encoded into the dithering patterns of an original image on the document, then at step 24 the digital signature is extracted from the dithering patterns of the same image on the document and the document key is recovered using the public key for the document. If the document key was printed on the physical media then at step 24 the document key is read from the document. If the digital signature was printed on the document then at step 24 the digital signature is read from the document being authenticated and the document key is recovered using the public key for the document. Alternatively, shared secret keys, i.e. symmetric keys, may be used.

At step 26, the recovered document key obtained at step 24 is compared to the document key generated at step 20. If the document keys match at step 28 then the document is verified as authentic at step

30. Otherwise, the document is not verified as authentic at step 32.

The private key secures the image to the underlying paper. This may be used to generate checks for originality. An authorized copy may be created where a new original/copy may be produced using the public key to decode the document key of the original. The watermark may then be removed and then a new watermark re-encoded using the new document key which is signed with the private key.

Figure 4 shows one possible arrangement for generating a document key 52 for a document 40. This arrangement may be employed when authenticating the document 40 at step 10 and/or when verifying the document 40 at step 20. The document 40 is fed into an imager 42. The imager 42 generates a set of pixel values on an output 50. The pixel values on the output 50 are provided to a document key generator 44 which in response generates the document key 52 for the document 40.

The pixel resolution of the imager 42 is selected to enable detection of the unique physical attributes of the underlying paper of the document 40 upon which the document key 52 is based. In one embodiment, the imager 42 provides a pixel resolution of 2400 dots per inch which enables detection of the random differences in the density of the paper fibers that were formed during the manufacture of the paper that underlies the document 40.

In some embodiments, the document key generator 44 examines the pixel values in one or more predetermined areas of the document 40. There may be any number of these predetermined areas. The predetermined areas may be of any size and may be located anywhere on the document 40.

Figure 5 shows one possible arrangement of predetermined areas 60-62 of the document 40 which are examined by the document key generator 44. In this embodiment, the predetermined areas 60-62 are referenced by distances from an edge 70 and an edge 72 of the document 40. For example, corresponding edges of the predetermined area 60 are a distance d2 and a distance d1 from the edges 70 and 72, respectively. Similarly, corresponding edges of the predetermined area 62 are a distance d4 and the distance d1 from the edges 70 and 72, respectively.

In some embodiments, a box may be used to delineate the area to be scanned. The box may be given orientation features (for example, directionality) to aid the reader in extracting the document key. Multiple boxes may be used for additional security and tolerance to document damage.

The document key generator 44 may use any encoding method for generating the document key 52. For example, the document key generator 44 may generate a checksum of the pixel values in each of the predetermined areas 60-62 and then determine an average of the checksums to yield the document key 52. As another example, the document key generator

44 may employ an MD5 encoding technique on the pixel values in the predetermined areas 60-62 to generate the document key 52.

In some embodiments, the document key 52 for the document 40 may be recorded in, for example, a data base along with information that describes what is originally printed on the document 40. Thereafter, the document 40 may be authenticated by obtaining its document key and performing a data base lookup using the document key to obtain the information that describes what was originally printed on the document 40. If something else is printed on the document 40 then it can be concluded that the original printing was stripped and replaced by a forger.

A flourescent or ultraviolet (uv) source of the appropriate wavelength may be used to with a uv sensor to detect a reflective substance or UV ink in the document 40. The uv ink or reflective substance is preferably imparted into the document 40 during manufacture of the underlying paper media so as to render it difficult and expensive for a forger to duplicate. The uv ink may be put into threads of the paper media. The reflective areas of the document 40 may be printed.

The foregoing detailed description of the present invention is provided for the purposes of illustration and is not intended to be exhaustive or to limit the invention to the precise embodiment disclosed. Accordingly, the scope of the present invention is defined by the appended claims.

CLAIMS

What is claimed is:

1. A method for authenticating a document, comprising the steps of:

generating a document key by examining one or more physical attributes of a physical media that underlies the document;

imparting an original image onto the physical media such that the original image enables recovery of the document key.

2. The method of claim 1, wherein the step of imparting comprises the steps of:

generating a digital signature using the document key and a private key that corresponds to the document;

encoding the digital signature into the original image.

3. The method of claim 1, wherein the step of imparting comprises the step of printing the document key on the physical media as the original image.

4. The method of claim 1, further comprising the step of recording the document key along with a description of the document.

5. The method of claim 1, further comprising the step of verifying the document by performing the steps of:

generating the document key by examining the physical attributes of the physical media;

obtaining a recovered document key from the original image;

comparing the document key to the recovered document key.

6. The method of claim 1, wherein the step of generating a document key comprises the step of examining paper fiber patterns in the physical media.

7. The method of claim 6, wherein the step of examining paper fiber patterns comprises the step of examining paper fiber patterns in each of a set of predetermined areas of the physical media.

8. The method of claim 1, wherein the step of imparting comprises the steps of:

generating a digital signature using the document key and a shared secret key that corresponds to the document;

encoding the digital signature into the original image.

9. The method of claim 1, wherein the physical media is paper.

10. The method of claim 1, wherein the step of generating a document key comprises the step of examining density differences of the physical media.

11. The method of claim 1, wherein the step of generating a document key comprises the step of

examining a unique pattern imparted in the physical media.

12. The method of claim 11, wherein the step of examining a unique pattern comprises the step of examining a pattern of a reflective substance in the physical media.

13. The method of claim 11, wherein the step of examining a unique pattern comprises the step of examining a pattern of UV ink in the physical media.

14. The method of claim 11, wherein the step of examining a unique pattern comprises the step of examining a set of predetermined shapes printed in predetermined positions on the physical media.

15. The method of claim 14, further comprising the steps of measuring the predetermined positions and encoding the predetermined in the document key.

16. An apparatus for authenticating a document, comprising:

imager that generates a set of pixel data values in response to a document;

document key generator that generates a document key by examining the pixel data values to detect one or more physical attributes of a physical media that underlies the document thereby enabling the document key to be imparted in an original image onto the document.

17. An apparatus for authenticating a document, comprising:

imager that generates a set of pixel data values in response to a document;

document key generator that generates a document key by examining the pixel data values to detect one or more physical attributes of a physical media that underlies the document thereby enabling the document key to be compared to a recovered document key obtained from the document.

ABSTRACT

A method for authenticating a document in which a document key for the document is generated by examining one or more attributes of a physical media that underlies the document. An original image is then imparted onto the physical media so that the original image is associated with the document key in a way that enables a subsequent recovery of the document key from the original image. This tying together of the underlying physical media, through the document key, with an original image enables detection of a forgery which was performed either through an alteration of the original image, or ink stripping and re-printing, or a printing of the original image on another physical media.

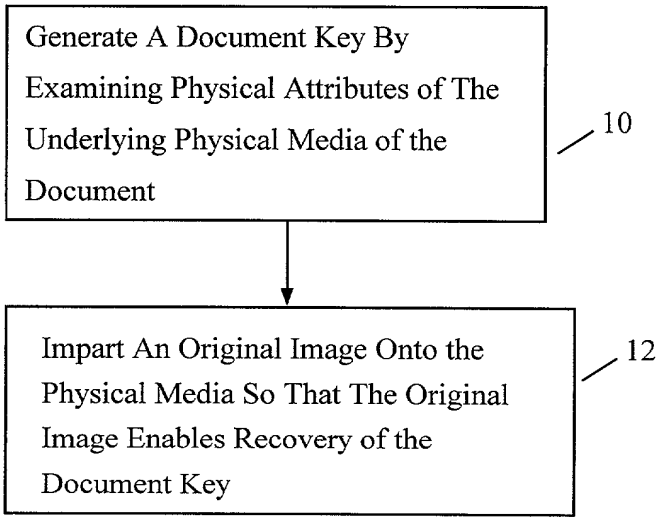

Generate A Document Key By Examining Physical Attributes of The Underlying Physical Media of the Document
10
Impart An Original Image Onto the Physical Media So That The Original Image Enables Recovery of the Document Key
12

FIG. 1

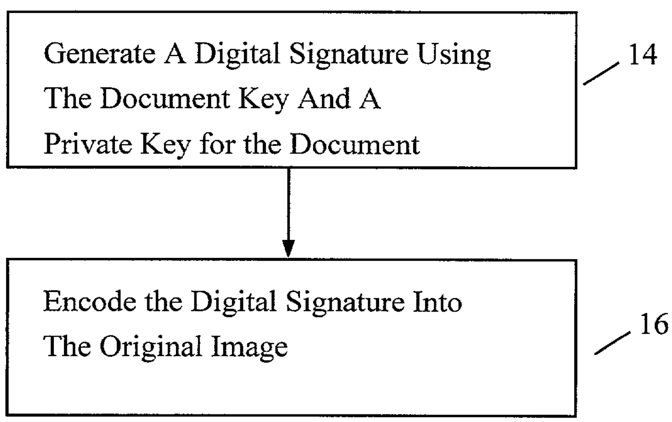
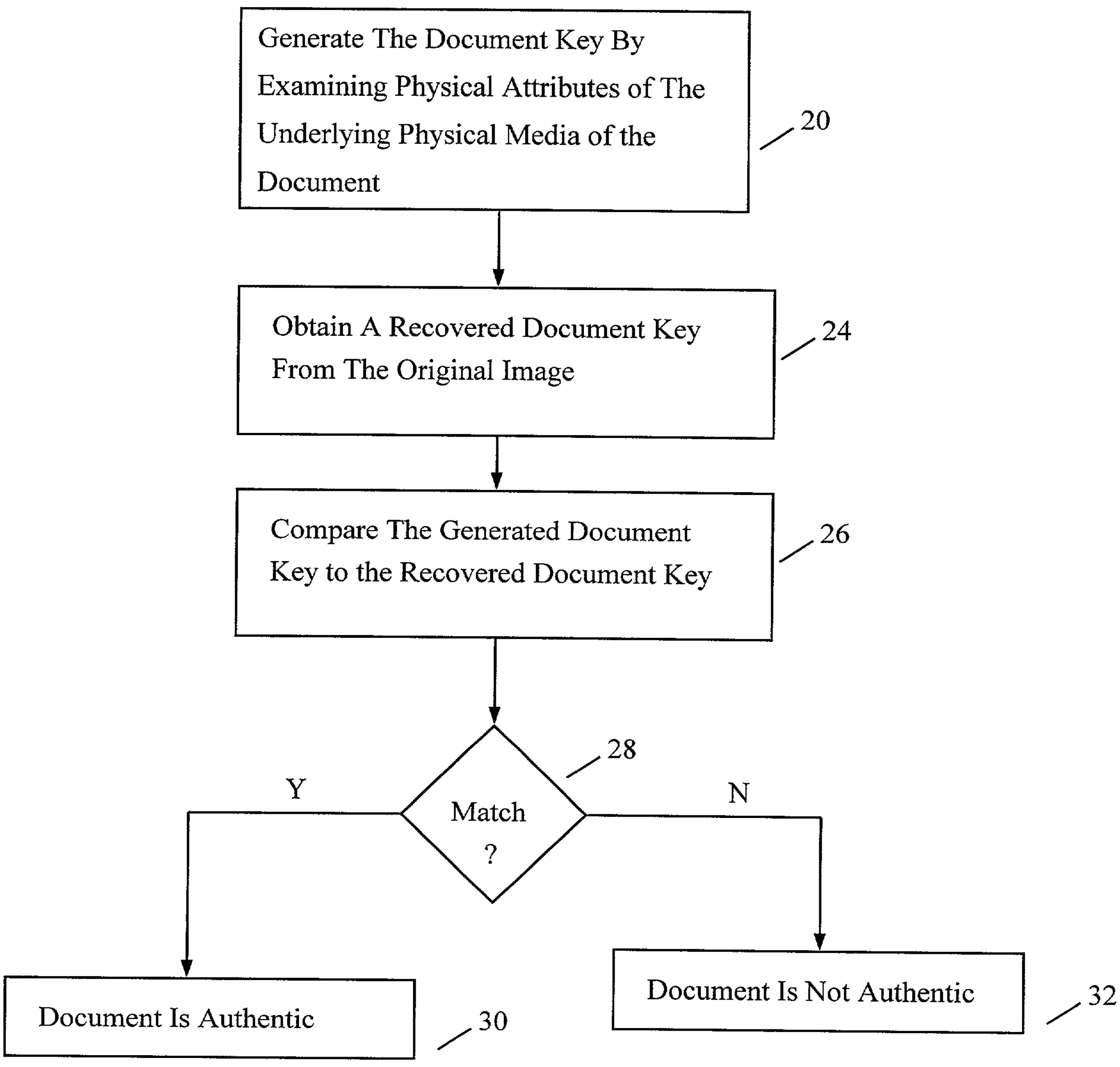

Generate A Digital Signature Using
The Document Key And A
Private Key for the Document
14
Encode the Digital Signature Into
The Original Image
16

FIG. 2



10992596

FIG. 3

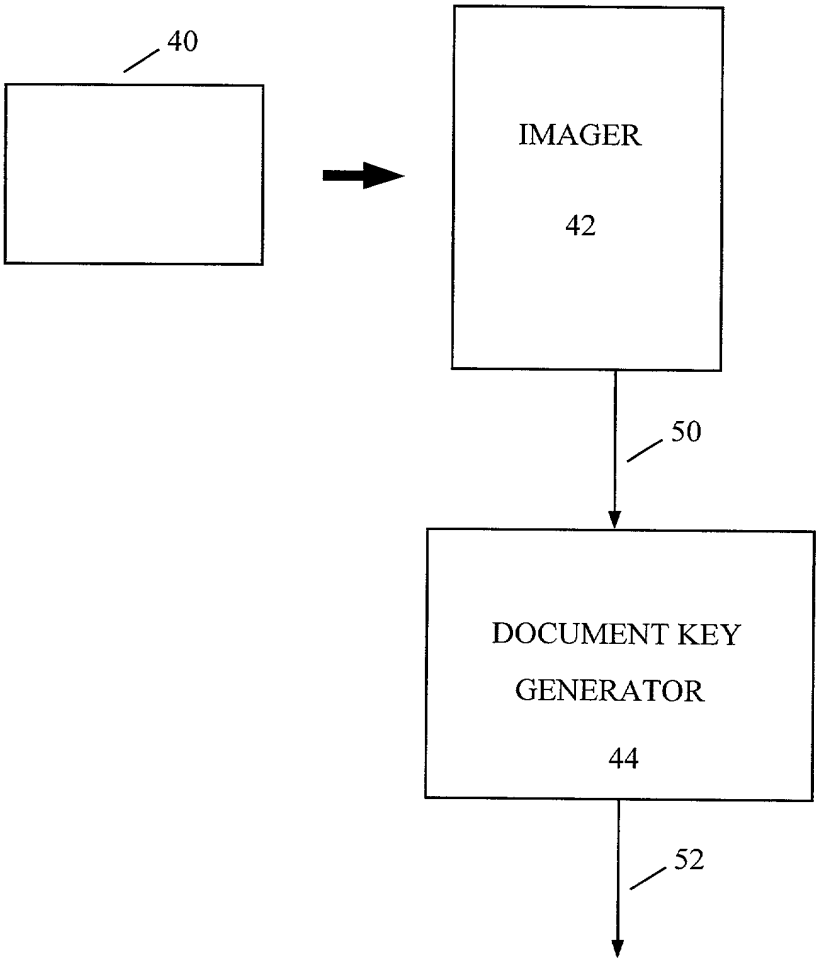


FIG. 4

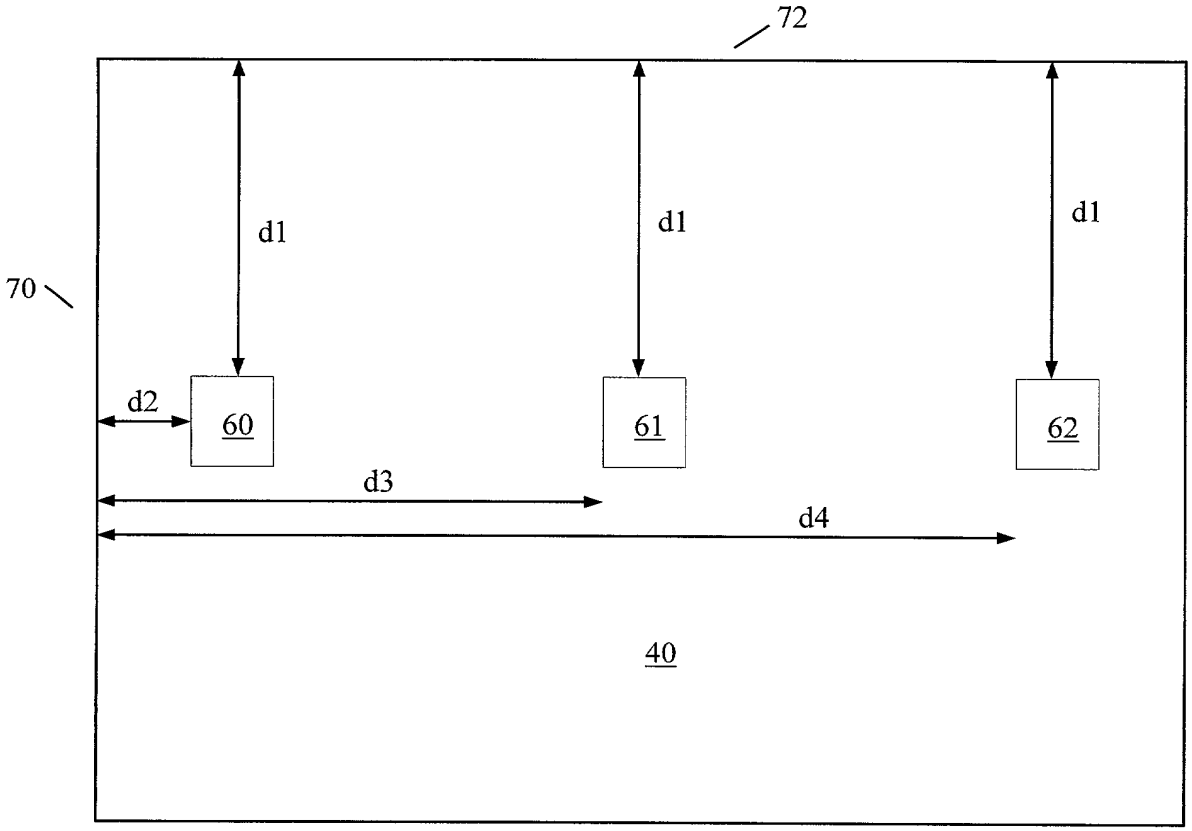


FIG. 5

10992596

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

ATTORNEY DOCKET NO. 10992596-1

As a below named inventor, I hereby declare that:

My residence/post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Document Authentication Using the Physical Characteristics of Underlying Physical Media

the specification of which is attached hereto unless the following box is checked:

( ) was filed on _____ as US Application Serial No. or PCT International Application Number _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understood the contents of the above-identified specification, including the claims, as amended by any amendment(s) referred to above. I acknowledge the duty to disclose all information which is material to patentability as defined in 37 CFR 1.56.

Foreign Application(s) and/or Claim of Foreign Priority

I hereby claim foreign priority benefits under Title 35, United States Code Section 119 of any foreign application(s) for patent or inventor(s) certificate listed below and have also identified below any foreign application for patent or inventor(s) certificate having a filing date before that of the application on which priority is claimed:

COUNTRY	APPLICATION NUMBER	DATE FILED	PRIORITY CLAIMED UNDER 35 U.S.C. 119
N/A			YES: ___ NO: ___
			YES: ___ NO: ___

Provisional Application

I hereby claim the benefit under Title 35, United States Code Section 119(e) of any United States provisional application(s) listed below:

APPLICATION SERIAL NUMBER	FILING DATE
N/A	

U. S. Priority Claim

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION SERIAL NUMBER	FILING DATE	STATUS (patented/pending/abandoned)
N/A		

POWER OF ATTORNEY:

As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith:

Customer Number 022879

Place Customer Number Bar Code Label here

Send Correspondence to:
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80528-9599

Direct Telephone Calls To:
Thomas X. Li
(650) 857-5972

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Inventor: Keith E. Moore **Citizenship:** US

Residence: 3090 Mauricia Avenue, Santa Clara California 95051

Post Office Address: Same

Keith Edward Moore
Inventor's Signature

October 30, 2000
Date